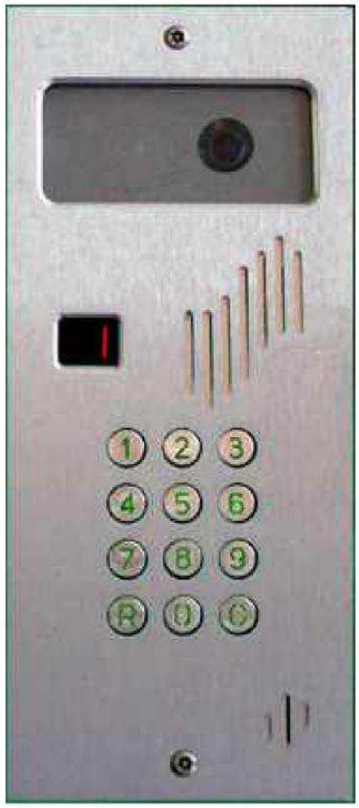


City Access
Video-citofono IP SIP std.
Manuale Utente

Ver. 1.5, Maggio 2015

ING. GIANNI SABATO
Via S. Stefano 74, I-40125 Bologna
GSM +39 335 238046
Ph. +39 051 6211553
Fax +39 051 3370960
E-mail: info@doingsecurity.it
Web: www.doingsecurity.it

Assistenza tecnica Tel.: +39 329 2288344 / +39 051 6211553

Tel.: +39 335 238046 ✉ : info@doingsecurity.it

Indice

1 Introduzione

Il videocitofono IP CITY ACCESS è stato sviluppato per essere connesso in LAN (local area network, cioè una rete locale di un edificio cablata o con connessioni wi-fi) oppure per essere utilizzato in WAN (wide area network, cioè in Internet) e agisce come un dispositivo VOIP a standard SIP.

Con il termine "*remote user agent*" ci si riferisce ad un dispositivo audio/video VOIP capace di connettersi in remoto con il video-citofono IP.

Ogni *user agent* audio/video compatibile SIP dovrebbe essere in grado di comunicare con il video-citofono City Access. Questo è valido da un punto di vista teorico, perché non può essere garantita una totale compatibilità con tutti i dispositivi SIP di mercato e in alcuni casi non si escludono cattive qualità di comunicazione con alcuni *user agent* specifici: è pertanto fortemente consigliato di verificare la compatibilità in termini di qualità di connessione audio/video con lo *user agent* che si intende utilizzare.

Si raccomanda di utilizzare l'applicazione *Linphone* (ref. www.linphone.org, disponibile per PC Windows e come applicazione sia iOS che Android), un telefono software open-source, quale *remote user agent* in alternativa agli hardware di mercato a standard SIP. È anche disponibile una APP specifica per terminali Android.

Per quel che riguarda l'invio di comandi da parte del *remote user agent*, si faccia riferimento ai comandi "DTMF" (Dual Tone Modulated Frequency) che, agendo come una tastiera virtuale, realizzano codici per aperture di porte e cancelli; è anche possibile usare messaggi SIP quali carrier di codici DTMF, selezionando nelle impostazioni del *remote user agent* "send DTMF as sip info". In opzione, nella gamma City Access è anche disponibile un video-terminale SIP da interno che utilizza i messaggi SIP (modello "SOTTILE").

Una cura particolare è stata riservata nella realizzazione del software per contrastare eventuali bugs. I software complessi, come quello sviluppato per il video-citofono CITY ACCESS, dispongono di watch-dog per controllare costantemente l'attività del software stesso. Questo permette una affidabilità di lungo termine, ma non evita brevi periodi di inattività (durata inferiore ai 30 secondi), nei rari casi in cui il watch-dog necessita di agire per il ripristino della funzionalità.

Si noti che il processo di configurazione è stato progettato per limitare il rischio di vulnerabilità, sia contro attacchi malevoli che nel caso di blocchi di funzionamento causati da operazioni non corrette di persone non qualificate.

I codici PIN di accesso possono essere usati per aprire il varco tramite l'uso della tastiera integrata nel video-citofono: questi codici sono memorizzati in forma criptata tale che sia impossibile rilevarli anche accedendo ai file di sistema. Tutti i PIN possono essere facilmante modificati tramite il codice PIN master - anch'esso memorizzato in forma criptata.

Questo manuale descrive un dispositivo che, come tutti i dispositivi tecnologici, è in continuo sviluppo: visto che la gamma City Access aderisce allo standard SIP, non dovrebbero esserci rischi di incompatibilità con le precedenti versioni.

1.1 Organizzazione del presente manuale

Il presente Manuale Utente è diviso in sezioni. Il capitolo "Descrizione Prodotto" fornisce le principali prestazioni tecniche del CITY ACCESS. Il capitolo "Funzionamento Utente di Base" descrive l'uso giorno per giorno del video-citofono.

La sezione "Installazione Software" fornisce indicazioni di setup avanzate per la configurazione e l'attivazione del CITY ACCESS.

La sezione "Installazione Hardware" descrive come installare l'unità CITY ACCESS.

Infine in "Appendice" vengono fornite informazioni di impostazione utili ai system integrator.

NOTA.

In questo manuale non è descritto alcun hardware da interno (video-telefoni, smartphone o software PC): CITY ACCESS è sviluppato per essere compatibile con il più ampio numero di dispositivi a standard SIP possibile.

Durante il tempo di boot (circa 30 secondi) il dispositivo non è pronto per effettuare chiamate (i segmenti del display lampeggiano durante il boot). Per i modelli di video-citofono senza display, lampeggiano i LED bianchi della telecamera invece che i segmenti rossi del display.

1.2 Terminologia

- **Ethernet -** tecnologia di comunicazione per la realizzazione di reti di computer in ambito locale (LAN)
- **LAN -** rete locale, rete di computer per un'area di piccole dimensioni, per es. un ufficio, un'abitazione o un gruppo di edifici come una scuola o un aeroporto
- **10Base-T -** 10 Mbit/s, usa un connettore modulare a 8 vie, generalmente chiamato RJ45, nell'ambito Ethernet con coppie twistate. I cavi generalmente usati sono a 4 coppie twistate (sebbene 10BASE-T e 100BASE-TX usino solamnete due di tali coppie). Ciascun stardard supporta la comunicazione sia full-duplex che half-duplex. Operano su distanze fino a 100 metri
- **100Base-TX -** noto come **Fast Ethernet**, usa due coppie UTP o STP, CAT5
- **Coppia Twistata -** è un cablaggio nel quale due conduttori sono twistati insieme per cancellare l'interferenza elettromagnetica (EMI) proveniente da sorgenti esterne, per esempio la radiazione elettromagnetica da cavi non schermati, e il crosstalk da coppie poste nelle vicinanze
- **UTP**, Unshielded Twisted Pair - coppia twistata non schermata
- **STP**, Shielded Twisted Pair - coppia twistata schermata; uno schermo metallico è posto attorno a ciascuna coppia per proteggere il cavo da interferenze elettromagnetiche (EMI)
- **WEB -** World Wide Web (WWW), applicazione del protocollo internet HTTP
- **HTTP -** Hypertext Transfer Protocol; è un protocollo internet usato originariamente per lo scambio di documenti ipertestuali in formato HTML

- **USB -** Universal Serial Bus; metodo per la connessione seriale di dispositivi esterni al computer
- **Video codec** - compressione **H.263** derivata da MPEG-4, **H.264** è un codec per il formato AVC MPEG-4. **MPEG-4** è un tipo di compressione video
- **JPEG** è un metodo standard di compressione usato per salvare immagini digitali
- **Voice over Internet Protocol** (**VoIP**) è una tecnologia che permette la trasmissione di voce digitalizzata all'interno di paccetti del protocollo **UDP/TCP/IP** nelle reti di computer. È usato per effettuare telefonate via Inernet, Intranet o altri tipologie di connessioni dati
- **TCP/IP** contiene un set di protocolli per la comunicazione nelle reti di computered è il protocollo principale di Internet
- **IP address** è un numero che identifica chiaramente una interfaccia nella rete di computer che usa il protocollo IP
- **DHCP** (Dynamic Host Configuration Protocol) è un protocollo della famiglia TCP/IP. È usato per assegnare automaticamente indirizzi IP a singoli PC nelle reti di computer, semplificando il lavoro dell'amministratore di rete
- **Internet** è un sistema di reti di computer connessi a livello mondiale
- **Intranet** è una rete di computer simile a Internet, ma di tipo privato. Questo significa che è usata esclusivamente da un gruppo di utenti limitato (es. Una azienda e le sue filiali)
- **PoE** (Power over Ethernet) è un sistema di alimentazione attraverso il cavo di rete che non necessita di ulteriori cablaggi per la fornitura di energia elettrica
- **NTP** (Network Time Protocol) è un protocollo per la sincronzzazione degli orologi interni ai computer
- **DTMF** (dual tone multi frequency) is the signal to the phone provider that is generated when pressing an ordinary telephone's touch keys.

2 Descrizione Prodotto

CITY ACCESS è un avanzato e flessibile video-citofono a standard SIP.

Dispone di una tastiera retroilluminata e di un display a due caratteri per far sì che si possano chiamare fino a 99 diversi indirizzi sip (cioè fino a 99 differenti numeri di interno).

Grazie ad un robusto pannello frontale in alluminio e a un tettuccio parapioggia, il video-citofono può essere installato sia ad incasso che su muro.

CITY ACCESS ha due relè da 8A e tre uscite open collector - tutte queste uscite possono essere attivate dai terminali SIP installati all'interno dell'edificio, quali per esempio video-telefoni, smartphone, tablet e PC.

Le principali prestazioni tecniche del CITY ACCESS sono elencate nella tabella che segue.

□ TDati tecnici / Prestazioni	
Chipset CPU chipset	Architettura ARM11, BCM2xxx, frequenza clock 700 MHz, co-processore Dual Core GPU
Memoria	512 MBytes
Interfacce	1x 10/100 Ethernet RJ45, 2x USB, 1x SD card
Tastiera retroilluminata	12 tasti (cifre 0 ... 9 e tasti "C", "R") per selezionare max 99 interni / accosso PIN
Lettore TAG	Lettore EM / Mifare / NFC opzionale (upgrade futuro)
Ingressi / Uscite	2x relè NA / NC 8A @ 250Vca, 3x open collector (200 mA; 1A di picco per tempi inferiori a 1 ms)
Alimentazione	10 ~ 15 Vcc; consumo: max 900 mA @ 12Vcc; tip. 400 mA
Display	2-cifre a 7-segmenti
Video	H263+; H264 (upgrade futuro)
Telecamera	640 x 480 pixels con illuminatore a LED bianchi
Audio	Codec G722
Standard	Compatibilità con protocollo SIP
Housing	Pannello frontale anti-vandalo spessore 10 mm, uso esterno
Dimensioni e peso	Pannello frontale: 120 (L) x 270 (A) x 10 (P) mm; 1200 g Box plastico da incasso: 118 (L) x 262 (A) x 65(P)
Temperatura di lavoro	Da -10°C a +50°C, U.R. Fino al 90% senza condensazione
Opzioni	Tetto parapioggia; unità Legenda; lettore RFID

3 Funzionamento Utente di Base

3.1Come effetuare una chiamata

Per effettuare una chiamata, immettere il numero da chiamare (uno o due cifre) e premere il pulsante "C".

> NOTA.
>
> Per i video-citofoni che dispongono di pulsanti di chiamata diretta (modelli CTA01.1B, CTA01.2B, CTA01.3B e CTA01.4B), premere semplicemente il pulsante associato all'interno da chiamare. Il presente Manuale va riferimento al modello CTA01.CL che dispone di tastiera integrata.

Ogni numero è associato ad uno o più indirizzi SIP (vd. Paragrafo seguente).

Dopo aver premuto il pulsante "C", il numero dell'estensione chiamata inizierà a lampeggiare nel display e verrà chiamato il primo indirizzo SIP associato. Se questo indirizzo SIP non è online, allora sarà chiamato il secondo e così via.

Se il numero chiamato è online, l'altoparlante emetterà i tipici suoni della chiamata telefonica finché l'interno non risponde.

Se il numero interno rifiuta la risposta, per esempio l'utente rigetta la chiamata o non risponde in tempo, CITY ACCESS automaticamente abortirà la chiamata corrente. Il tempo massimo per effettuare la risposta alla chiamata è definito dal parametro "timeout sec ua confirmed" contenuto nel file slvdp.ini (vd. Sezione "Setup mediante l'uso di una chiavetta USB").

Una chiamata può essere interrotta anche dal visitatore in ogni momento premendo il tasto "R".

Se il *remote user agent* risponde in tempo, il diplay a due cifre interromperà il lampeggio e l'altoparlante interromperà l'emissione dei toni di chiamata. L'illuminatore verrà acceso e la connessione verrà stabilita. Sulla base delle scelte da parte del *remote user agent* , il video può essere abilitato oppure no. Abilitare il solo audio può essere la soluzione ideale nel caso di connessione a Internet con larghezza di banda limitata. Per connessioni in LAN, non dovrebbero esserci problemi con la disponibilità di banda per il video e, in tal caso, la connessione video può essere abilitata senza problemi.

Il tempo massimo di una conversazione è definito dal parametro "timeout sec ua disconnected".

3.2 Ricerca automatica del remote user agent

Come anticipato nei paragrafi precedenti, ogni numero digitato nella pulsantiera può essere associato a più di un indirizzo SIP da chiamare (vd. Descrizione file **slvdp.sip**). Si possono associare fino a 3 indirizzi SIP allo stesso numero di pulsantiera.

Quando un visitatore chiama un numero di interno seguito dal pulsante "C", gli indirizzi SIP associati vengono chiamati in sequenza finché non viene trovato un *remote user agent* in linea. Questo meccanismo di ricerca automatica permette facilmente di modificare il *remote user agent* che deve rispondere ad una chiamata, per esempio semplicemente attivando una APP su uno smartphone.

Supponiamo di avere un video-terminale interno (*remote user agent*), installato su un muro della casa, e che si voglia rispondere con uno smartphone per evitare che qualcuno in casa venga disturbato dai suoni di chiamata (per esempio un bambino che dorme) o semplicemente si desideri ricevere la chiamata in un altro posto, quando si è lontani da casa o se si desidera simulare la presenza in casa.

Per essere in grado di rispondere al posto del video-terminale interno, basta semplicemente attivare la APP sullo smartphone - per esempio con la APP dedicata CTA o con una APP freeware (per es. Linphone). Quando la APP dello smartphone viene nuovamente disattivata, allora il video-citofono City Access chiama il video-terminale interno.

Gli scenari tipici dove avere un vantaggio da questa funzionalità sono:

- Il vostro bambino o qualcuno sta dormendo in casa e non si vuole che il video-termianale interno suoni creando disturbo
- Siete seduti sul divano e preferite rispondere alla chiamata e - nel caso - aprire la porta senza dovervi muovere
- Siete lontani dal video-terminale interno, per esempio seduti nel giardino dietro casa, e potreste non avere la possibilità di sentire i toni della chiamata del video-citofono ma solo quelli dello smartphone o del dispositivo (PC / tablet) che state usando
- Un amico è in ritardo all'appuntamento ma dovete uscire di casa per recarvi in un altro luogo: attivando la APP sul vostro smartphone sarete in grado di rispondere alle chiamate che giungono dal video-citofono
- Si desidera simulare la presenza nella vostra abitazione, nel caso un malitenzionato chiamasse al video-citofono per verificare la vostra presenza
- Si ha la necessità di doversi allontanare dalla propria casa per un imprevisto, ma si prevede che qualcuno dovrà venire a trovarvi e non ne conoscete il numero di telefono per informarlo

3.3 Come aprire una porta / cancello

La persona che risponde alla chiamata (*remote user agent*), può facilmente aprire un cancello o una porta, digitando un codice che dovrà corrispondere a quanto programmato nel file **slvdp.sip**. Notare che questo codice può essere programmato per essere lungo da una sola cifra a più cifre:

per default il tasto 1 è associato al relè 1, il tasto 2 al relè 2 e così via per tutte e 5 le uscite (il City Access ha due relè e 3 uscite open collector).

È anche possiile attivare le uscite a partire dalla tastiera integrata del CITY ACCESS. Se necessario, un codice PIN può essere associato a ciascuna uscita cosicché un utente autorizzato può attivare l'uscita desiderata mediante un codice PIN da digitare sulla tastiera del CITY ACCESS.

Per commutare un'uscita, seguire i passi seguenti:

- Premere il tasto "R"
- Premere 4 volte il tasto "C": il display mostrerà l'indicazione "P1"
- Digitare il codice PIN associato all'uscita che si desidera attivare
- Premere il tasto "R"
- Se il codice PIN immesso è accettato, l'uscita verrà commutata per aprire la porta / cancello

Per default nessun codice PIN è abilitato, quindi è impossibile aprire l'accesso immettendo una qualunque sequenza numerica.

Per impostare o modificare uno dei codici PIN, deve essere utilizzato il codice PIN Master: per default questo codice PIN è "987654" e anch'esso può essere modificato.

> NOTA.
>
> Notare che il codice PIN Master di default dovrebbe essere modificato subito dopo l'installazione del video-citofono CITY ACCESS: questo per ragioni di sicurezza contro accessi non-autorizzati.

I codici PIN per attivare le uscite a partire dalla tastiera del video-citofono CITY ACCESS devono rispondere alle regole seguenti:

- La prima cifra si riferisce al numero di uscita (quindi tutti i codici PIN che iniziano con la cifra "1" attivano il relè 1, tutti i codice PIN che iniziano con "2" attivano il relè 2 e così via fino all'uscita no.5)
- Tutti i codice PIN devono avere un minimo di 2 cifre e non devono avere più di 8 cifre
- Come esempio, 199234 può essere un codice PIN valido per aprire l'accesso no.1 e 297266 può essere un codice valido per aprire l'accesso no.2
- Un codice PIN lungo una sola cifra, disabiliterà la possibilità di usare codici PIN per aprire porte e cancelli su quel numero di uscita: per esempio il codice PIN "1" disabiliterà la possibilità di attivare il relè 1 a partire dalla tastiera del CITY ACCESS
- Il codice PIN Master deve sempre iniziare con la cifra "9": per esempio un codice PIN Master valido può essere 913357.
- Il codice PIN Master deve essere lungo almeno due cifra e non può avere più di 8 cifre.

> NOTA.
>
> Inserendo per due volte il carattere "0" invece che un nuovo PIN, il display mostrerà la scritta "PP" e inizierà una nuova sessione di setup da tastiera: far riferimento al paragrafo "Setup usando la tastiera del dispositivo" per ulteriori informazioni.

Per impostare o modificare un codice PIN (incluso il codice PIN Master) eseguire i seguenti passi di programmazione:

- Premere il tasto "R"
- Premere per 4 volte il tasto "C": il display mostrerà l'indicazione "P1"
- Immettere il codice PIN Master che inizia con la cifra "9" (il codice PIN Master di default è "987654")
- Premere il tasto "C": il display mostrerà l'indicazione "P2"
- Digitare il nuovo codice PIN (lungo da 2 a 8 cifre) che inizia con "1" per il PIN dedicato all'uscita no.1, "2" per l'uscita no.2, ... e che inizi con la cifra "9" per la modifica del codice PIN Master
- Premere il tasto "C": il display mostrerà l'indicazione "P3"
- Digitare nuovamente il nuovo codice PIN per verifica
- Premere il tasto "C": il display mostrerà per un momento l'indicazione "PA" per segnalare che il nuovo codice PIN è stato accettato. Altrimenti il display mostrerà "PE" per indicare uno stato di errore: in questo caso premere il tasto "R" e ripetere la procedura sopra descritta perché il codice PIN immesso non è stato memorizzato.
- Se il display mostra l'indicazione "PC", questo significa che il codice PIN è stato disabilitato per quell'uscita.

Esempio 1: impostare il codice PIN 34455 per l'uscita no.3 usando il codice PIN Master di default

- Premere il tasto "R"
- Premere 4 volte il tasto "C": il display mostrerà "P1"
- Digitare il codice PIN Master di default 987654
- Premere il tasto "C": il display mostrerà "P2"
- Digitare "34455"
- Premere il tasto "C": il display mostrerà "P3"
- Digitare nuovamente "34455"
- Premere il tasto "C": il display mostrerà "PA" per qualche istante

Esempio 2: modificare il codice PIN Master a 911346 dal valore di default

- Premere il tasto "R"
- Premere 4 volte il tasto "C": il display mostrerà "P1"
- Digitare il codice PIN Master di default 987654
- Premere il tasto "C": il display mostrerà "P2"
- Digitare "911346"
- Premere il tasto "C": il display mostrerà "P3"
- Digitare nuovamente "911346"
- Premere il tasto "C": il display mostrerà "PA" per qualche istante

4 Installazione Software

4.1 Setup usando la tastiera del dispositivo

Il CITY ACCESS permette di tarare i parametri acustici usando la tastiera integrata nel dispositivo.

> NOTA.
>
> Questa prestazione non è disponibile per i modelli CTA01.1B, CTA01.2B, CTA01.3B e CTA01.4B (video-citofoni con pulsanti di chiamata diretta verso gli interni).

Per entrare nella modalità setup usando la tastiera, effettuare i passi seguenti:

- Premere il tasto "R"
- Premere 4 volte il tasto "C": il display mostrerà "P1"
- Digitare il codice PIN Master (per default 987654)
- Premere il tasto "C": il display mostrerà "P2"
- Premere "0" e il tasto "C": il display mostrerà "P3"
- Premere "0" e il tasto "C": il display mostrerà "PP" per indicare che la tastiera può essere usata per tarare i principali parametri acustici (vd. Figura 4.1).

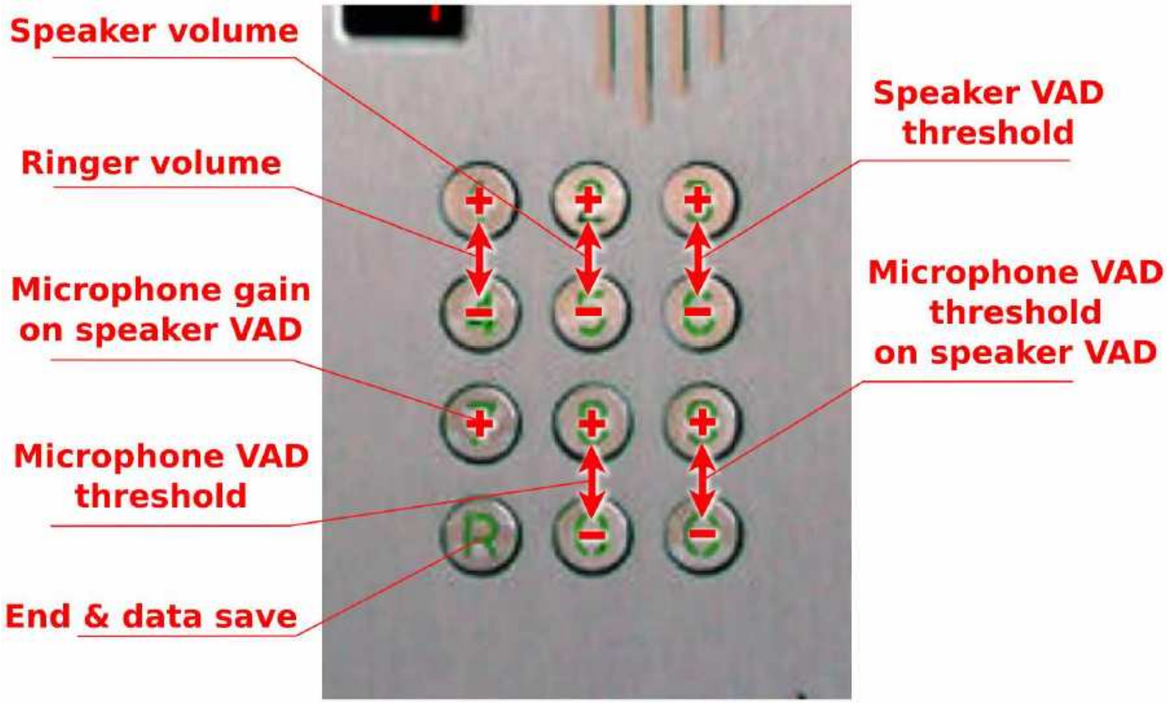


Fig. 4.1. *Taratura parametri acustici usando la tastiera*

Non appena viene premuto un tasto, il valore del parametro corrispondente è mostrato nel display al posto dell'indicazione "PP": il parametro può essere tarato usando i tasti +/- come da figura 4.1 precedente. Tutti i parametri hanno due tasti (SU/GIU) con l'eccezione del valore del parametro "microphone gain on speaker VAD" che ha un tasto singolo e che ciclicamente assumerà i valori da 1 a 8.

Se non viene premuto alcun tasto per un certo tempo, sul display comparirà nuovamente "PP" ad indicare che si è in una sessione di setup mediante tastiera dei parametri acustici.

Per uscire dalla sessione di setup, può essere premuto il tasto "R" o si può attendere il timeout: uscindo dal modo setup, il display tornerà OFF (modo operativo normale).

Il setup mediante tastiera permette di tarare i seguenti parametri:

- **Ringer volume -** permette di tarare il volume dei suoni di chiamata e goni volta che si aumenti o si diminuisca il livello del volume, viene emesso un breve tono che permette di avvertire il volume selezionato.
- **Speaker volume -** permette di modificare il volume voce in uscita all'altoparlante.
- **Speaker VAD threshold** - permette di pulire la voce dall'altoparlante dal rumore di fondo durante le pause della comunicazione audio
- **Microphone gain on speaker VAD** - permette di decrementare il guadagno del microfono durante l'attività voce. Questo parametro dovrebbe essere tenuto al valore massimo, se non ci fossero altri sistemi per eliminare l'effetto eco.
- **Microphone VAD threshold** - permette di evitare l'invio di rumore di fondo verso il *remote user agent* quando un visitatore durante la chiamata interrompe il parlato. Questo parametro permette di pulire l'audio.

- **Microphone VAD threshold on speaker VAD** - permette di incrementare la soglia VAD del microfono durante il parlato e questo permette efficacemente di evitare eco non voluti senza sacrificare la sensibilità del microfono agento sul guadagno del microfono stesso.

> NOTA.
>
> L'acronimo VAD significa "voice activity detector". Si noti che il setup di fabbrica dei parametri precedenti dovrebbe essere tale da adattarsi alla maggior parte delle applicazioni, così da evitare di doverli modificare sul sito se non eccezionalmente.

4.2 Setup mediante l'uso di una chiavetta USB

Il setup di fabbrica può essere facilmente modificato attraverso file di testo. Questi files devono essere contenuti nella cartella chiamata **slvdp** (notare che devono essere usate lettere minuscole), creata nella directory root di una chiavetta USB che deve essere formattata **vfat** (il modo di formattazione tipico del sistema operativo Windows).

Non è necessario caricare nella chiavetta files che non devono essere modificati: inserire nella chiavetta USB solo i file oggetti di modifica, tutti contenuti nella cartella slvdp.

Per caricare i file di setup, è necessario inserire saldamente la chiavetta USB in una porta disponibile nella scheda del City Access prima di fornire alimentazione al video-citofono. L'estrazione della chiavetta USB può avvenire quando il display si spegne ad indicare il termine del processo di setup.

> NOTA.
>
> Per i video-citofoni City Access senza il display (modelli CTA01.1B, CTA01.2B, CTA01.3B e CTA01.4B) è necessario attendere 60 secondi per permettere il completamento del processo di setup prima di estrarre la chiavetta USB.

Dopo che il processo di setup si sia completato nella chiavetta USB si troveranno copia di tutti i file sostituiti durante il processo rinominati con il prefisso **slvdp**. Questo permette di ristabilire facilmente la configurazione precedente, se necessario.

Nei paragrafi seguenti si può trovare una descrizione dettagliata dei files di configurazione.

4.2.1 File slvdp.ini

Contiene i valori di configurazione di diversi parametri del video-citofono. Una doppia barra (slash) introduce un commento. Notare che il parametro "sip domain" è automaticamente impostato a local ip, se non specificato diversamente. Visto che i parametri di audio / video in uscita sono oggetto di negoziazione con il *remote user agent*, le impostazioni audio / video di uscita possono essere selezionate nelle preferenze del *remote user agent*. Modifiche a questo file non sono normalmente richieste. Tenere un campo vuoto significa che il programma utilizzerà il valore di default per quel parametro.

```
sip user = vdp                    // default: "vdp"
```

sip domain = mydomain.com // default: detected ip address
sip password = // default: null string (no password)
upd port = 5060 // default: 5060
rtp audio port = 4000 // default: 4000
rtp video port = 5000 // default: 5000
video width = 352 // default: 176 pixel
video height = 288 // default: 144 pixel
video fps = 8 // default: 8 frame per second
video quality avg = 300 // average video encoding quality
video quality max = 500 // max video encoding quality
timeout sec ua early = 6 // max time to find remote user in seconds, default: 6
timeout sec ua confirmed = 30 // max time remote user from ringing to answer in seconds, default: 30
timeout sec ua disconnected = 60 // max connection time with remote user agent in seconds, default: 60
tsec relay on = 1 // relay activation time in seconds: min 0, max 14, default 2
tsec to autoreset = 30 // max time keyboard idle before autoreset in seconds: range 0..127 sec, default 30
nr push to password = 4 // number of “C” key pushes to enable password access: value can range from 1 to 6, default 3
beep attenuation = 2 // ring volume: value can range from 0=laud, to 10=quiet
beep extended = 1 // extends ringing to initial search before connection in seconds: default 0
send dtmf as info = 1 // 0 send as dual tone, 1 (default) send as sip info
// leave unchanged following parameters (advance settings)
video fps d = 1 // frame per second divisor (default 1)
render width = 704 // width of local video (incoming) image: 0 to use default settings
render height = 576 // height of local video (incoming) image
audio sample per frame = 80 // min: 64, max: 256, default: 80
kill incoming video = 0 // 0 accept, 1 kill (warning: killing can result in unstable behaviour)
kill rendering = 1 // 0 render incoming video on local screen, 1 kill
restart program = 7 // 1 after incoming calls, 2 after outgoing calls, 3 always
h264 priority = 1 // 0 disables H264, 1 (default) enables H264 with low priority

4.2.2 File slvdp.sip

Contiene la lista degli indirizzi SIP da chiamare, terminati dal carattere #. Ogni linea corrisponde al numero di interno selezionato nella tastiera del video-citofono (numero ad una o due cifre, da 1 a 99) eseguito dal visitatore che vuole chiamare un utente: quindi la prima riga del file slvdp.sip elenca gli indirizzi SIP da chiamare quando viene premuto il pulsante "1" seguito dal pulsante "C"

sul video-citofono CITY ACCESS, la seconda riga elenca gli indirizzi SIP da chiamare quando viene premuto il pulsante "2" seguito dal pulsante "C" sul video-citofono CITY ACCESS, e cosi via fino alla 99ma riga. Come esempio, si faccia riferimento all'elenco sotto riportato:

sip:mario@192.168.1.103 & sip:user2@192.168.1.107 & sip:jane@192.168.1.109
sip:smith@192.168.1.12 - 2 - 1 - 3 - 4 - 5
#
Comments ...

In questo esempio, quando il visitatore preme il pulsante "1" seguito dal pulsante "C" sulla tastiera del CITY ACCESS, verrà chiamato per primo l'indirizzo sip:mario@192.168.1.103 e, se questo non risultasse online, verrà chiamato l'indirizzo sip:user2@192.168.1.107 e infine l'indirizzo sip:jane@192.168.1.109, qualora anche il secondo indirizzo fosse offline.

Dopo il carattere # è possibile scrivere un commento in una forma qualsiasi.

Ogni riga dell'elenco di indirizzi SIP deve iniziare con un indirizzo SIP valido (chiamato “sip uri”) nella forma: sip:<user>@<ip> o sip:<user>@<domain_name>. Se viene usato un nome dominio allora è necessario registrare l'indirizzo IP su un provider sip uri.

È possibile scrivere fino a 3 indirizzi SIP sulla medesima riga, divisi dal carattere &. Tutti gli indirizzi SIP della stessa riga sono associati al medesimo numero da chiamare (da 1 a 99) e quando sarà digitato quel numero, gli indirizzi SIP del rigo corrispondente saranno chiamati in sequenza finché uno di essi non verrà trovato online.

Questo meccanismo di ricerca automatico permette facilmente di cambiare il *remote user agent* associato al numero chiamato, attivando / disattivando una APP di uno smartphone.

Il numero associato all'indirizzo SIP è il numero di riga dove è localizzato quell'indirizzo nel file. Non sono ammesse linee vuote nell'elenco degli indirizzi SIP: solo nella parte commenti è possibile avere righe vuote.

Per aprire un accesso a partire dal dispositivo interno (*remote user agent*, es. video-telefono SIP, smartphone, PC, ...) è necessario digitare sulla tastiera del *remote user agent* il numero dell'uscita (da 1 a 5: 1 e 2 per le due uscite a relè, 3, 4 e 5 per le uscite open collector). Per default le uscite possono essere attivate da una singola cifra che corrisponde al numero dell'uscita stessa: 1, 2, 3, 4, 5.

Se questa logica deve essere alternata, allora dopo l'indirizzo SIP è possibile elencare i comandi di apertura che devono essere dati attraverso la tastiera del video-telefono o del PC: il carattere '-' dopo l'indirizzo SIP introduce le cifre da usare per attivare le uscite. Al massimo si possono definire 5 comandi sulla stessa riga per il medesimo indirizzo SIP. Nell'esempio riportato sopra, l'indirizzo sip:smith@192.168.1.12 aprirà l'accesso corrispondente al relè 1 digitando la cifra 2.

I comandi numerici di apertura devono essere scritti concordemente la sequenza delle porte di uscita, ciò significa che la prima cifra è relativa al primo relè, la seconda al secondo relè, la terza all'uscita open collector n.3, e così via.

Sono ammesse solo cifre per i comandi di apertura.

4.2.3 File interfaces

Contiene il setup dell'indirizzo IP locale, file che sarà modificato in "interfaces.installed" dopo la rimozione della chiavetta USB a processo di setup concluso. La presenza di tale file forza un processo di riavvio (reboot) per far sì che le modifiche apportate siano effettive.

Deve essere configurato per essere compatibile con la rete nella quale il video-citofono è connesso. Si deve prestare attenzione nel cambiare questo file perché influisce sul file di configurazione Linux presente nella cartella /etc/network/ folder.

Per una piena comprensione su questo file, si prega di leggere le pagine del manuale Linux "/etc/network/interfaces", facilmente scaricabile da Internet.

Una configurazione base di queso file è simile alla seguente:

```
auto lo
iface lo inet loopback
#iface eth0 inet dhcp
iface eth0 inet static
   address 192.168.1.99
   netmask 255.255.255.0
   network 192.168.1.0
   broadcast 192.168.1.255
   gateway 192.168.1.1
allow-hotplug wlan0
iface wlan0 inet manual
wpa-roam /etc/wpa_supplicant/wpa_supplicant.conf
iface default inet dhcp
```

Potrebbe essere necessario modificare i parametri seguenti: indirizzo IP, rete IP, broadcast IP e gateway IP per rendere il video-citofono compatibile con la rete dove verrà installato. Se è utilizzata una rete separata, non dovrebbero esserci ragioni particolari per cambiare questi indirizzi.

4.2.4 Setup via rete con ssh

Un accesso remoto al video-citofono è possibile con SSH (secure shell) purché questo sia stato abilitato come descritto nel paragrafo "Setup mediante l'uso di una chiavetta USB".

Dopo il setup, si raccomanda di proteggere il video-citofono da accessi remoti malevoli disabilitando ssh. Alternativamente si raccomanda di cambiare la password amministratore di default.

Per l'accesso SSH, la porta da utilizzare deve essere 65022. L'indirizzo IP di default del video-citofono è 192.168.1.99.

Per default, il login amministratore è:

User: **root**

Password: **raspi1234**

Per utenti Linux, l'accesso amministratore via SSH si ottiene aprendo un terminale e digitando al prompt comandi:

ssh -o port=65022 root@192.168.1.99

(sustituire 192.168.1.99 con l'indirizzo IP scelto se i valori di setup sono stati modificati)

Per utenti MAC, può essere utilizzando un client SSH chiamato Terminal così da connettersi a server remoti. Per default, Terminal.app è localizzato nella cartella Applications -> Utilities. Eseguire un doppio-click sull'icona per avviare il client e poi digitare il comando:

ssh -o port=65022 root@192.168.1.99

Per le piattafrome Windows si può utilizzare l'applicativo freeware Putty (ssh client) - Putty può essere libaramente scaricato da Internet, per esempio all'indirizzo http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

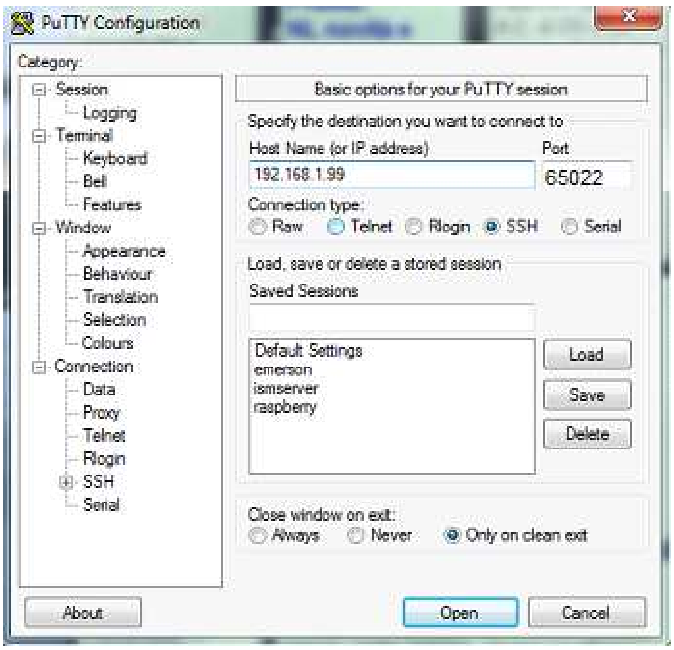


Fig. 4.2. *Putty access*

Per utenti Android, un semplice client SSH può essere scaricato dallo store Google alla pagina https://play.google.com/store/apps/details?id=apc.android.tool.telnet

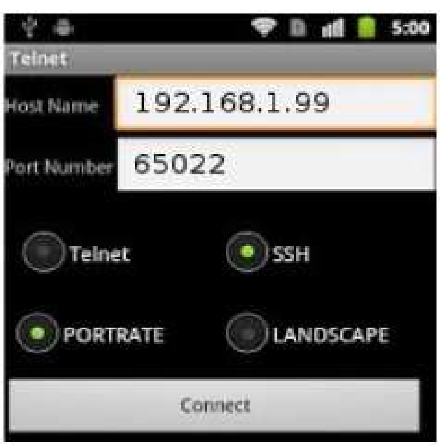


Fig. 4.3. *APP Android telnet*

Siccome per tablet e smartphone sono disponibile le sole connessioni WiFi, potrebbe essere richiesto un adattatore USB-Ethernet. Notare che non tutti i dispositivi Android hanno il supporto nativo di tali adattatori.

Dopo avere effettuato il login quale amministratore, tutti i i file di configurazione sono accessibili nella cartella /home/pi/vdp - quindi la linea di comando deve essere

cd /home/pi/vdp

dove "**cd**" significa cambia directory.

Altri comandi utili sono:

- **ls -** comando per elencare i file
- **mv filename_old filename_new -** comando per muovere un file o cambiargli nome
- **nano filename -** comando per editare un file

I cambiamenti diventano effettivi solo dopo un reboot del video-citofono. Per forzare il reboot, inviare un comando di halt come root. Il watch dog interno effettuerà un reboot in automatico.

4.2.5 Remote user agent, configurazione preferenze

Sebbene il City Access possa gestire diversi codec, la qualità di connessione risultante può essere fortemente influenzata da questa scelta.

Raccomandiamo di selezionare G722 quale codec audio e H263-1998 quale codec video (codec anche noto come H263+), cif (352x288) o qcif (176x144) quale risoluzione video preferenziale.

4.3 Watch-dog per effettuare cicli di auto-reboot

CITY ACCESS include una piattaforma Linux e un controllo che agisce da watch-dog. Questo controlla costantemente se il programma principale è vivo, gestendo eventuali problemi quali: stop o bocchi di programma, degrado del sistema sul lungo periodo. Un blocco di programma fa sì che il software venga immediatamente rilanciato e venga automaticamente eseguito un auto-reboot.

L'auto-reboot assicura che il video-citofono sarà riavviato in uno stato iniziale noto, con RAM pulita e recuperando tutti i memory leaks causati da un possibile sistema degradato. L'esecuzione del watch dog dura meno di 30 seconds per ristabilire pienamente la funzionalità del sistema. Durante il processo di watch dog il display mostra la scritta "CC" e poi la scritta lampeggiante "--" finché non si abbia il ciclo di ripristino completato.

4.4 Registrazione con server SIP registrar (SIP provider)

Affinché il CITY ACCESS sia registrato ad un provider SIP, è necessario modificare il file "/home/pi/vdp/keepalive.sh" - vd. Appendice. Si può eseguire questa modifica usando un client ssh, come descritto al paragrafo 4.2.4.

Si deve aggiungere alla linea di avvio del CITY ACCESS (./slvdp...) gli argomenti seguenti:

```
--id sip:alice@example.com --registrar sip:example.com \
--realm * --username alice --password secret
```

Questo farà sì che il CITY ACCESS sia registrato sul server sip:example.com usando la ID utente *alice* e la password *secret*. Tutti gli argomenti della linea di comando sono obbligatori.

Alcune spiegazioni circa i comandi descritti sopra sono qui sotto riportati:

--id sip:alice@example.com	Imposta l'identificazione dell'utente e sarà utilizzato nell'intestazione *From:* di tutte le richieste inviate da CITY ACCESS
--registrar sip:example.com	Imposta l'indirizzo del server dove saranno inviare le richieste REGISTER
--realm example.com	Il *realm* delle credenziali per autenticarsi verso il server. Il valore qui indicato DEVE essere in match con il realm inviato dal server nelle intestazioni WWW-Authenticate o Proxy-Authenticate nella risposta 401/407. In alternativa possono essere utilizzate wildcard (*) perché PJSIP risponda ad ogni realm
--username alice	Imposta la username di autenticazione. Normalmente il valore è lo stesso della parte username dell'intestazione *From:*, ma ciò non è necessario per il CITY ACCESS
--password secret	Imposta la password per l'autenticazione

> NOTA.
>
> L'impostazione realm deve essere in match con il realm del challenge altrimenti si verificherà un errore PJSIP_ENOCREDENTIAL. Se il realm non è noto, utilizzare wildcard (*) quale realm per far sì che PJSIP risponda ad un qualsiasi realm.

CITY ACCESS supporta inoltre identità multiple e registrazioni a diversi server. Per registrarsi simultaneamente sia al provider1.com e al provider2.com:

```
--id sip:bob@provider1.com --registrar sip:provider1.com \
--realm provider1.com --username bob --password secret \
--next-account \
--id sip:bob@provider2.com --registrar sip:provider2.com \
--realm provider2.com --username bob --password secret
```

Per registrarsi al server example.com con identificativo utente *alice* e inviare le richieste a outbound.home.com che richiede una autenticazione differente:

```
--id sip:alice@example.com --registrar sip:example.com \
--proxy outbound.home.com \
--realm example.com --username alice --password secret --next-cred \
--realm outbound.home.com --username blah --password blahblah
```

Notare che il programma del CITY ACCESS (slvdp) è una versione modificata del programma open source *pjsua* e quindi anche CITY ACCESS viene rilasciato nei termini GPL. Le informazioni fornite in questa sezione sono già fornite dal programma open source *pjsua* a cui il programma slvdp aderisce.

> NOTA.
>
> Nel caso di utilizzi Asterisk, si suggerisce di far riferimento alla guida online:
>
> https://wiki.asterisk.org/wiki/display/AST/Asterisk+PJSIP+Troubleshooting+Guide

5 Installazione Hardware

5.1 Connessioni hardware

Il dispositivo fornisce una serie di uscite che vengono associate ai comandi descritti nel file **slvdp.sip**. Ogni comando di apertura commuterà una di queste uscite per un tempo programmabile indicato nel file **slvdp.ini** dal parametro "tsec relay on" (default: 1 secondo).

Comando 1 (dal terminale interno) o codice PIN 1 commutano l'uscita RL1

Comando 2 (dal terminale interno) o codice PIN 2 commutano l'uscita RL2

Comando 3 (dal terminale interno) o codice PIN 3 commutano l'uscita UOC-X9-2 a GND

Comando 4 (dal terminale interno) o codice PIN 4 commutano l'uscita UOC-X9-4 a GND

Comando 5 (dal terminale interno) o codice PIN 5 commutano l'uscita UOC-X9-6 a GND

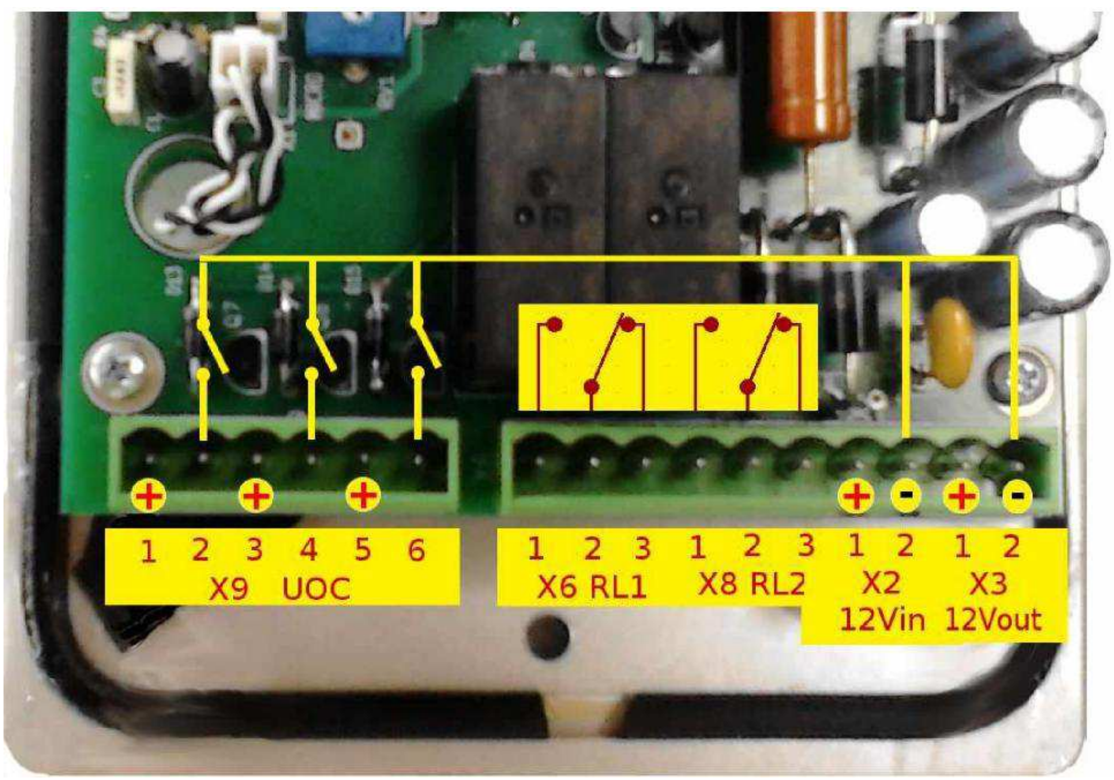


Fig. 5.1. *Connessioni I/O*

Il video-citofono deve essere alimentato con tensione ai pin 12Vin. Un buffer con un circuito di dumping circuit viene fornito per supportare picchi di corrente elevati ai morsetti 12Vout, così da poter alimentare bobine di apriporta senza influenzare troppo l'alimentazione. Ciò significa che si può richiedere una minor corrente ai pin 12Vin.

Il dispositivo richiede circa 500 mA di assorbimento ma si deve considerare un carico medio aggiuntivo degli apriporta elettromeccanici a cui connettere le uscite.

La tensione di ingresso può variare da 10Vcc a 15Vcc.

Attenzione!

Una tensione oltre i 16Vcc applicata ai pin di ingresso 12Vin può causare in danni ingenti del video-citofono e perfino causare l'esplosione delle capacità.

Il range di alimentazione permette una connessione diretta a batterie convenzionali 12V al piombo perché agiscano quali UPS in caso di mancanza di alimentazione. Il CITY ACCESS può inoltre agire come carica-batteria se il connettore X2 (12Vin) è alimentato con una tensione da 14Vcc e una batteria al piombo acido a 12V è connessa direttamente a X3 (12Vout).

Attenzione!

Un carica batteria appropriato deve essere utilizzato e deve essere scelto affinché non risulti mai che anche una accidentale connessione faccia sì che la tensione ecceda i 16Vcc all'ingresso 12Vin, anche per un breve periodo di tempo.

5.2Schemi circuitali

Gli schemi seguenti mostrano alcuni dettagli circuitali utili come riferimento.

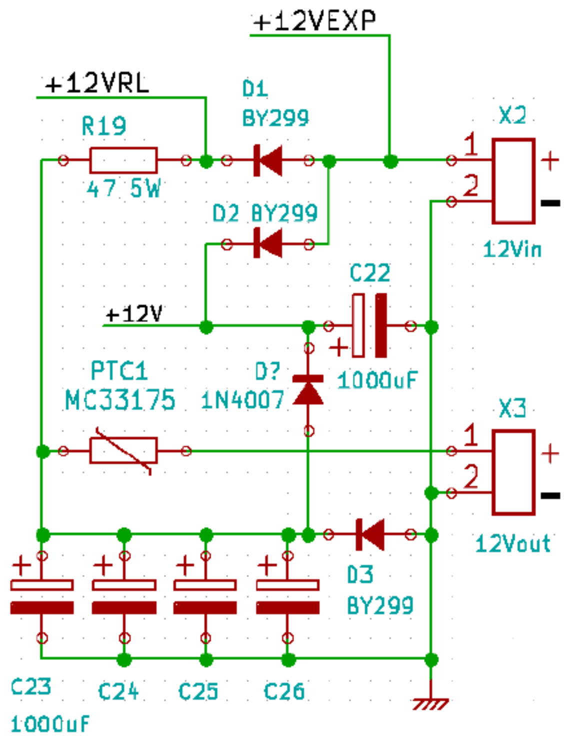


Fig. 5.2. *Schema circuitale 1*

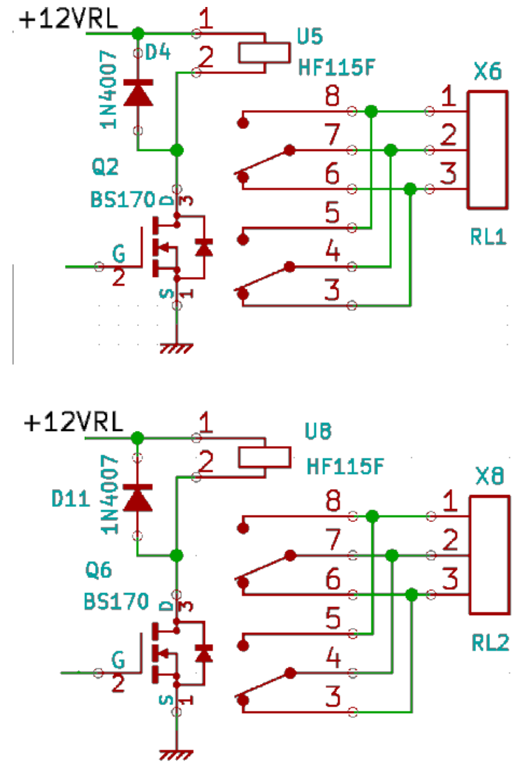


Fig. 5.3. *Schema circuitale 2*

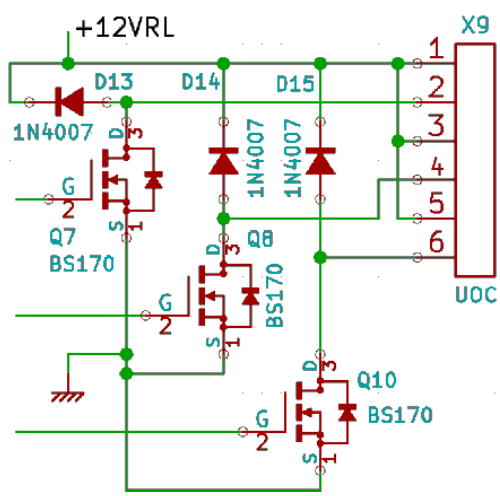


Fig. 5.4. *Schema circuitale 3*

NOTA.

Considerare che gli schemi precedenti sono solo di riferimento visto che sia l'hardware che il software sono in continuo miglioramento, il che potrebbe modificare gli schemi circuitali senza preavviso.

5.3Specifiche elettriche

Descrizione	Valore
Alimentazione	10 - 15V CC
Tensione massima assocula ai pin12Vin	16 V CC (nota 1)
Consumo corrente - tip	400 mA (nota 2)
Consumo corrente - picco corto-circuito	10 A
Consumo corrente - corto-circuito lunga durata	150 mA (nota 3)
Carico max relè (corrente e tensione)	8 A @ 250 V CA
Uscita Open drain - max coorente continua	200 mA (nota 4)
Uscita Open drain - max I di picco per t <1ms	1 A (notea4)
Temperatura di lavoro	-10 °C ~ +50 ℃

Note

1) Una tensione superiore a 16Vcc applicata ai morsetti 12Vin può causare danni ingenti al dispositivo e causare l'esplosione di capacità. Se è usata una batteria di backup, deve essere previsto un appropriato carica batterie on-line e deve essere scelto tale da evitare accidentali false connessioni che possano risultare in una tensione di ingresso superiore a 16Vcc anche se per pochi istanti di tempo.
2) Condizioni: pin 12Vout aperti, display off, LED bianchi off
3) La corrente su 12Vout è limitata da una resistenza di potenza da 82 ohm
4) Attenzione! Non è fornita alcuna protezione di corto-circuito sulle uscite open drain! (UOC X9)

6 Configurazioni tipiche

Tipicamente il CITY ACCESS può essere utilizzato in tre diverse tipologie di sistema:

- **Abitazioni residenzioni -** in questo tipo di applicazioni, il CITY ACCESS ha un link diretto alla LAN dell'abitazione attraverso uno switch o usando un Access Point.
- **Condomini o edifici multi-utente -** se il video-citofono CITY ACCESS è utilizzato come un controllo accesso ad un edificio, dove si suppone siano presenti molti utenti, è probabile che venga utilizzato un video-citofono con tastiera (modello CTA01.CL) così da permettere agli utenti autorizzati di accedere con un codice PIN e permettere ai visitatori di chiamare fino a 99 diversi interni - ognuno dei quali con il proprio *remote user agent*. Inoltre ciascun condomino è probabile abbia una sua linea ADSL e quindi si suppone di utilizzare un NAT (Network Address Translation) per ciascun appartamento / utente.
- **Edifici commerciali / industriali -** siti dove sono presenti accessi multipli ciascuno dotato di video-citofono per l'accesso e dove sono utilizzati centralini telefonici IP in rete locale (IP PBX opzionalmente offerti assieme alla gamma di prodotti CITY ACCESS).

Nei paragrafi seguenti sono descritti gli step di base di configurazione dei CITY ACCESS.

6.1 Abitazione residenziale

Nella figura che segue, viene mostrata una tipica installazione per una abitazione residenziale.



Fig. 6.1. *Architettura di sistema per abitazione residenziale*

Per una configurazione di una abitazione residenziale, si devono compiere i passi seguenti:

- Prendere nota dell'indirizzo IP del router: per esempio 192.168.1.1
- Editare il file **slvdp.sip** e inserire i seguenti indirizzi (accertarsi che gli indirizzi IP siano all'interno della stessa classe IP del router):
  - sip:indoor@192.168.1.90 & sip:mobile@192.168.1.70 //si suppone che il terminale interno da muro abbia l'indirizzo 192.168.1.90
- Scaricare dal sito www.doingsecurity.it la APP SipHome.apk per il dispositivo mobile e il plug -in video CSipSimple VideoPlugin.apk oppure usare il tablet 7" preconfigurato CTA01.TB
- Scaricare una APP per la configurazione dell'indirizzo IP sul dispositivo mobile, se necessario - per esempio **WiFi Settings**
- Cambiare il setup IP del dispositivo mobile all'indirizzo IP 192.168.1.70
- Usare la chiavetta USB per caricare i file da PC con le modifiche dei parametri City Access desiderati
- Editare il file **interfaces**:
  - Modificare - se necessario - l'indirizzo IP del video-citofono CTA01.1B (per default l'indirizzo del CITY ACCESS è 192.168.1.99)
- Editare il file **slvdp.ini**:
  - Modificare - se necessario - il tempo di attivazione del relè modificando il parametro "tsec relay on" (per esempio: tsec relay on = 3 per un'attivazione del relè di 3 secondi)
- Seguire la procedura descritta nel paragrafo 4.2 per caricare i cambiamenti sopra descritti nel video-citofono.

6.2 Edifici multi-utente

La figura seguente mostra una tipica architettura per un edificio multi-utente.

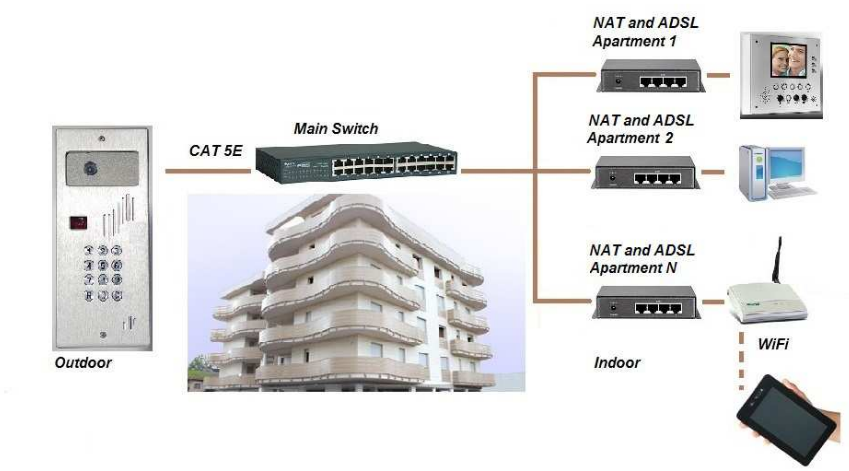


Fig. 6.2. *Architettura di sistema - Edificio condominiale*

Per un edificio condominiale, si suppone di avere un numero di utenti superiore a 4 tali per cui il modello di video-citofono più indicato è il CTA01.CL: questo video-citofono installato per esempio all'ingresso principale, permette anche di effettuare un accesso mediante codice PIN per gli utenti autorizzati. Si suppone anche che venga cablata una nuova rete. Per una configurazione di un impianto per un edificio come sopra raffigurato, si devono compiere i passi seguenti:

- Realizzare una rete locale indipendente (Cat 5E)
- Editare il file **slvdp.sip** come segue (si consiglia di usare un dispositivo NAT per ciascun appartamento così da rispettare l'indirizzo IP assegnato da ciascun router ADSL di ogni appartamento):
  - sip:apartment1@192.168.1.10
  - sip:apartment2@192.168.1.20
  - sip:apartment3@192.168.1.30
  - (...)
  - sip:apartment9@192.168.1.90 // ognuno degli indirizzi qui riportati è dedicato ad un utente
- Scaricare **Linphone** per PC Windows e impostarne l'indirizzo IP a 192.168.1.20
- Scaricare dal sito www.doingsecurity.it la APP SipHome.apk per il dispositivo mobile e il plug -in video CSipSimple VideoPlugin.apk oppure usare il tablet 7" preconfigurato CTA01.TB con le APP già installate
- Scaricare una APP per la configurazione dell'indirizzo IP sul dispositivo mobile, se necessario - per esempio **WiFi Settings**
- Cambiare il setup IP del dispositivo mobile all'indirizzo IP a 192.168.1.90
- Usare la chiavetta USB per caricare i file da PC con le modifiche dei parametri City Access desiderati
- Editare il file **interfaces**:
  - Modificare - se necessario - l'indirizzo IP del video-citofono CTA01.CL (per default l'indirizzo IP del CITY ACCESS è 192.168.1.99)
- Editare il file **slvdp.ini**:
  - Modificare - se necessario - il tempo di attivazione del relè modificando il parametro "tsec relay on" (per esempio: tsec relay on = 3 per un'attivazione del relè di 3 secondi)
- Seguire la procedura descritta nel paragrafo 4.2 per caricare i cambiamenti sopra descritti nel video-citofono.

6.3 Edifici commerciali / industriali

La figura seguente mostra una tipica architettura per un edificio commerciale / industriale.

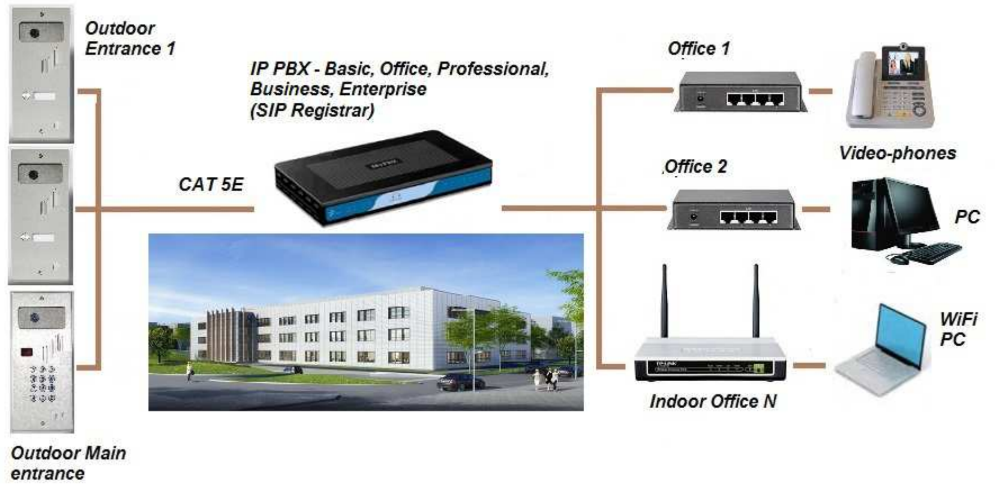


Fig. 6.3. *Architettura di sistema - Edificio commerciale / industriale*

In un impianto video-citofonico City Access per un edificio commerciale / industriale, si suppone di avere video-citofoni IP ai diversi accessi al sito e un IP PBX in rete LAN. La configurazione dell'impianto non si discosta da quanto descritto nei paragrafi precedenti; per quel che concerne il *SIP registrar*, seguire le istruzioni fornite nel paragrafo 4.4.

NOTA.

Qualora di desideri che un dispositivo mobile - smartphone o tablet - abbia la possibilità di rispondere, via internet, alle chiamate provenienti da un video-citofono CITY ACCESS, si consiglia l'utilizzo di un IP PBX - mod. Personal, Basic, Office o superiore - con l'utilizzo di un indirizzo SIP che comprenda il numero di telefono GSM (soluzione WAN).

7 Appendice

7.1 File ssh.enable

Il contenuto di questo file non ha importanza: la sua presenza abilita l'accesso ssh; ciò significa che si potrà essere in grado di aver accesso alla bash shell di Linux usando un client ssh da un PC connesso nella stessa rete. Suggeriamo l'uso di "putty".

7.2 File ssh.disable

Il contenuto di questo file non ha importanza: la sua presenza disabilita l'accesso remoto ssh. Questo è il comportamento di default dei video-citofoni City Access. Si tenga presente che un accesso remoto aumenta il rischio di attacchi malevoli di rete, così da rendere preferibile disabilitare l'accesso ssh se non fosse necessario, specialmente quando si è connessi a Internet.

7.3 File keepalive.sh

È uno script bash che lancia il programma slvdp mantenendolo in vita automaticamente in caso di crash di sistema.

```
#!/bin/sh
#
# this script indefinitely restart program when it stops working
# infinite loop
while [ 1 ]; do
   echo "slvdp launch.."
   ./slvdp --video --log-level=0 --max-calls=4 --auto-answer=200 --add-codec=G722
   sleep 1
done
exit 0
```

Il programma slvdp è lanciato con alcune opzioni che possono essere modificate, se richiesto. Per esempio, se si vuole effettuare chiamate SIP senza video, mantenendo solo la funzione audio, semplicemente evitare di includere l'opzione "--video" nella riga di comando.

7.4 SDK per integrazione con applicazioni OEM

Suggeriamo di riferirsi alle librerie Liblinphone:

http://www.linphone.org/eng/documentation/dev/liblinphone-free-sip-voip-sdk.html

http://www.belledonne-communications.com/liblinphone.html

Essendo Linphone un software open source, è possibile usare il suo codice sorgente per riferimento, sebbene ogni Software Development Kit SIP-compatibile potrebbe essere utilizzato. In alternativa raccomandiamo di usare i framework library del software open source Pjsip/Pjmedia.

Usando lo standard SIP e facendo riferimento a software open source, esiste una vasta gamma di opportunità per interfacciare i dispositivi City Access ad altri impianti.

7.5 Tracciamento dell’attività del City Access

È spesso necessario tracciare il comportamento del programma su un file di log, specie riguardo all’attività di rete. Lo strumento qui descritto costituisce un ottimo elemento per l’individuazione e la risoluzione di problemi di rete.

Nel seguito si suppone che l’indirizzo IP del dispositivo sia 192.168.1.99 (valore di default): nel caso, sostituire questo indirizzo con quello fornito al video-citofono in fase di configurazione.

Tener presente che l’attività di tracciamento del funzionamento del sistema carica il processore: pertanto alla fine dell’attività diagnostica è fortemente raccomandato di riavviare il video-citofono onde evitare che lavori in modo non ottimale. Pertanto alla fine della sessione SSH si raccomanda di inviare il comando:

sudo halt

Il City Access con il comando di halt effettuerà un reboot (con l’aiuto del watchdog) senza più generare l’attività di tracciamento. Questa procedura effettua anche la corretta espulsione della memoria USB che può venir rimossa senza provocare danni.

Per ottenere un file di log salvato su memoria USB, effettuare l’accesso SSH come utente “pi” (password “raspi”):

ssh -o port=65022 pi@192.168.1.99

Portarsi quindi nella cartella seguente:

cd /home/pi/vdp/

Immettere il comando seguente - tutto sulla medesima linea di comando:

sudo killall -9 slvdp && ./slvdp --video --log-level=3 --max-calls=4 --auto-answer=200 --add-codec=G722

Si può impostare il parametro --log-level da un valore 0 (bassa verbosità) fino a 5 (alta verbosità); il valore 3 è un buon compromesso per verificare l’attività di rete.

Il comando sopra riportato semplicemente ferma e riavvia il programma slvdp da remote terminal. Dopo aver inviato il comando si vedranno le tracce del programma sul terminale e non si potrà più inviare alcun ulteriore comando al video-citofono.

Per inviare altri comandi al City Access, per esempio per modificare il log-level, si deve aprire un altro terminale e connettersi via SSH come sopra descritto. L'invio del comando dal nuovo terminale rilascia la connessione al primo così che si possa essere in grado di inviare comandi ulteriori o stoppare la funzione diagnostica.

Nella maggior parte dei casi, si vorrà probabilmente salvare su un file di log le tracce che compaiono sul terminale SSH: questo può essere eseguito in modo differente in funzione del tipo di sistema operativo in uso.

Per utenti Linux, la registrazione dell'attivtià del terminale può essere eseguita semplicemente digitando il comando "script /whereyoulike/log.txt" prima di avviare la sessione SSH: il file di log (log.txt) sarà quindi creato nella cartella /whereyoulike/. Per ulteriori dettagli far riferimento al link seguente:

http://www.linuxandlife.com/2012/06/how-to-record-terminal-activities-and.html

Per utenti Windows, configurare PUTTY per registrare la sessione. Far riferimento a:

http://kb.site5.com/shell-access-ssh/putty-how-to-create-a-log-file-of-your-putty-session/

7.5.1 Registraizone log file su memoria USB

Creare una cartella chiamata "xlog" (in lettere minuscole) nella directory root di una memoria USB formattata come "vfat".

Inserire la memoria USB in una porta del City Access prima di accenderlo.

Eseguire un accesso remoto SSH come utente "pi" (password "raspi"):

ssh -o port=65022 pi@192.168.1.99

Ora installare la memoria USB con il comando:

sudo mount -t vfat -o uid=pi,gid=pi,rw,users,exec /dev/sda1 /home/pi/vdp/src

Controllare che la memoria USB sia stata correttamente installata (lo si può vedere nella cartella "xlog"):

ls /home/pi/vdp/src/

Ora cambiare la cartella corrente

cd /home/pi/vdp/

e digitare il comando su un'unica riga:

Sudo killall -9 slvdp && ./slvdp --video --log-level=5 --max-calls=4 --auto-answer=200 --add-codec=G722 > /home/pi/vdp/src/xlog/logfile1.txt

Le attività tracciate saranno normalmente attive solo durante una singola chiamata, così che il programma debba essere riavviato in modo "trace" prima di inizare una chiamata in debug.

Notare che il file "logfile1.txt" è un nome che può essere liberamente definito per creare il tracciamento dell'attività del video-citofono.

Il comando sopra descritto ferma e riavvia il programma slvdp dal terminale remot. Dopo aver inviato il comando non si potranno inviare ulteriori comandi al video-citofono (vedere le note sopra riportate al riguardo).

7.5.2 Lettura del log file

Un tipico file di log è qui sotto riportato.

Fase INVITE in cui, attraverso la porta 5060 viene mandato l'invito a collegarsi:

```
CSeq: 15597 INVITE
Contact: <sip:vdp@192.168.1.105:5060>
User-Agent: Linphone/3.5.0 (eXosip2/3.6.0)
Content-Length: 0
```

Passaggio alla fase EARLY in cui videocitofono squilla, e squilla anche Linphone:

```
13:43:45.523    pjsua_app.c  .....Call 0 state changed to EARLY (180
Ringing)
13:43:46.383          slvdp !>>>> ringing...
13:43:47.894          slvdp  >>>> ringing...
13:43:49.406          slvdp  >>>> ringing...
```

L'accettazione della chiamata da parte di Linphone con il messaggio 200 OK:

```
13:43:50.655   pjsua_core.c  .RX 670 bytes Response msg
200/INVITE/cseq=15597 (rdata0xd8590c) from UDP 192.168.1.105:5060:
SIP/2.0 200 OK
Via: SIP/2.0/UDP
192.168.1.99:5060;rport=5060;branch=z9hG4bKPjRciVLhwgcL2gM4Va2e-
hwFeRmiyfQEvo
From: <sip:192.168.1.99>;tag=c1FWz-.paJWxptmtQI4wRkKlFgHEwYpN
To: <sip:vdp@192.168.1.105>;tag=31918
Call-ID: SS0JoebARNLcqwn82ghWm9dyU9b3tA65
CSeq: 15597 INVITE
Contact: <sip:toto@192.168.1.105>
Content-Type: application/sdp
User-Agent: Linphone/3.5.0 (eXosip2/3.6.0)
Content-Length:   258
```

Risultato della negoziazione dei codec (vengono abilitati G722 e H263-1998 perchè sono i soli codec selezionati su Linphone):

```
v=0
o=toto 630 630 IN IP4 192.168.1.105
s=Talk
c=IN IP4 192.168.1.105
t=0 0
m=audio 7078 RTP/AVP 9 96
a=rtpmap:9 G722/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-11
m=video 9078 RTP/AVP 96
a=rtpmap:96 H263-1998/90000
a=fmtp:96 CIF=1;QCIF=1
```

Il riconoscimento dell'avvenuta connessione:

```
13:43:50.656    pjsua_app.c  .....Call 0 state changed to CONNECTING
 .......
13:43:50.662  pjsua_media.c  ......Audio updated, stream #0: G722
(sendrecv)
 .......
13:43:51.492  pjsua_media.c !......Video updated, stream #1: H263-1998
(sendrecv)
```

La chiusura della comunicazione a seguito della pressione tel tasto "abbassa cornetta" di Linphone:

```
13:44:19.945    pjsua_app.c  ......Call 0 is DISCONNECTED [reason=200
(Normal call clearing)]
 13:44:19.946 pjsua_app_comm  ......
   [DISCONNCTD] To: sip:vdp@192.168.1.105;tag=31918
     Call time: 00h:00m:28s, 1st res in 374 ms, conn in 6505ms
     #0 audio G722 @16kHz, sendrecv, peer=192.168.1.105:7078
        SRTP status: Not active Crypto-suite:
        RX pt=9, last update:00h:00m:08.218s ago
           total 1.4Kpkt 232.3KB (290.4KB +IP hdr) @avg=63.4Kbps/79.3Kbps
           pkt loss=0 (0.0%), discrd=1 (0.1%), dup=0 (0.0%), reord=0
(0.0%)
```

```
                (msec)     min      avg      max      last     dev
            loss period:   0.000    0.000    0.000    0.000    0.000
            jitter     :   1.250   25.944   83.000   20.500   10.915
         TX pt=9, ptime=20, last update:00h:00m:04.081s ago
            total 1.1Kpkt 173.8KB (217.9KB +IP hdr) @avg=47.4Kbps/59.5Kbps
            pkt loss=0 (0.0%), dup=0 (0.0%), reorder=0 (0.0%)
                (msec)     min      avg      max      last     dev
            loss period:   0.000    0.000    0.000    0.000    0.000
            jitter     :  15.750   19.469   22.000   19.875    1.667
         RTT msec      :  11.871  122.429  718.000   11.962   43.347
      #1 video H263-1998, sendrecv, peer=192.168.1.105:9078
         SRTP status: Not active Crypto-suite:
         RX pt=96, size=352x288, fps=25.00, last update:00h:00m:03.764s
ago
            total 1.8Kpkt 1.60MB (1.68MB +IP hdr) @avg=441.1Kbps/461.2Kbps
            pkt loss=0 (0.0%), discrd=1 (0.1%), dup=0 (0.0%), reord=0
(0.0%)
                (msec)     min      avg      max      last     dev
            loss period:   0.000    0.000    0.000    0.000    0.000
            jitter     :   0.133    7.361   14.877    4.422    3.307
         TX pt=96, size=352x288, fps=7.49, last update:00h:00m:01.267s ago
            total 589pkt 701.0KB (724.5KB +IP hdr)
@avg=192.4Kbps/198.8Kbps
            pkt loss=0 (0.0%), dup=0 (0.0%), reorder=0 (0.0%)
                (msec)     min      avg      max      last     dev
            loss period:   0.000    0.000    0.000    0.000    0.000
            jitter     :  14.400   19.321   29.311   26.944    4.564
         RTT msec      :   8.926  132.887  597.000   44.265   40.868
 13:44:19.946  pjsua_media.c  ......Call 0: deinitializing media..
 13:44:19.951  pjsua_media.c  ........Media stream call00:0 is destroyed
 13:44:19.951    pjsua_vid.c  ........Stopping video stream..
 13:44:20.022          slvdp !state changed to DISCONNECTED: call to nr.
5 uri >sip:vdp@192.168.1.105< correctly ended due to remote ua hang up
```

Si noti che alla chiusura della comunicazione vengono date anche molte informazioni relative al collegamento, sia per lo streaming audio che per lo streaming video. Si vedono chiaramente anche le porte utilizzate:

5060 per la negoziazione SIP
7078 per lo streaming audio (scelta in fase di negoziazione)
8078 per lo streaming video (scelta in fase di negoziazione)